Capstone Engagement Assessment, Analysis, and Hardening of a Vulnerable System

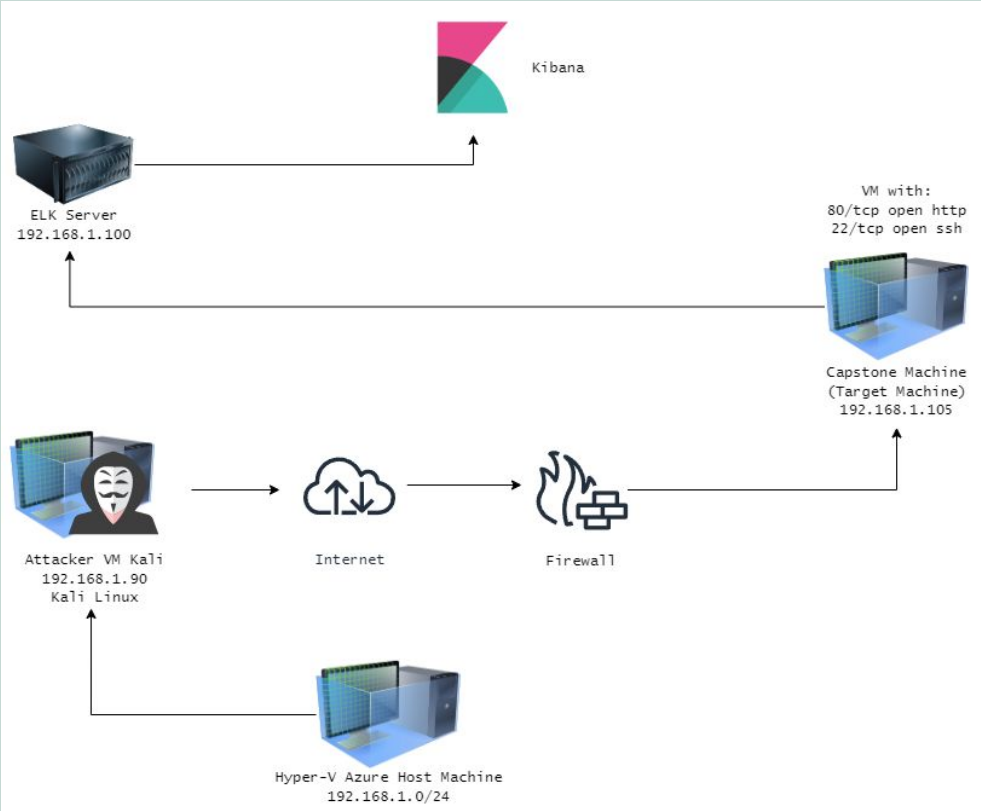
Yamilex Santiago-Rivera
University of Penn
Cybersecurity

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.76

Machines
IPv4: 192.168.1.105
OS: Windows 10
Hostname: Azure Hyper-V ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK-Stack

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure Machine ML-RefVM-684427	192.168.1.1	NATSwitch
Kali	192.168.1.90	Penetration Testing System
Capstone	192.168.1.105	Web Server
ELK	192.168.1.100	SIEM System

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Persistent Reverse Shell Backdoor	Able to deploy reverse shell payload exploit on web server as IPS/IDS/Firewall(s) allowing the outbound ports and undetected reverse shell.	Can gain remote backdoor shell access to Capstone Apache web server.
Weak Passwords and No Failed Password Lockout	Weak password was found in dictionary “rock you”. There were NO lockout for failed attempts allowing brute force attack.	The brute force was provide to: /secret_folder/ Password hash for Ryan dav://192.168.1.105/webdav/
CVE-2019-6579: 80/TCP	An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges and with network access to the affected service.	Successful exploitation of the security vulnerability compromises confidentiality, integrity or availability of the targeted system.
Directory Listing Enabled on Apache Web Server	Is able to use the browser to read full contents of directories on Capstone Apache web server.	Files were revealed, which shows Ashton as the administrator for the directory: /company_folders/secret_folder/

Exploitation: Nmap - Open Port 80

01

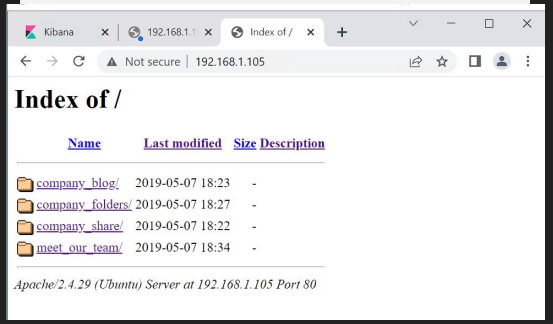
Tools & Processes

I exploited the vulnerability by using Nmap. An Nmap scan shows which ports are open and its service. In this case, when doing an Nmap scan, it showed that port 80/tcp and 22/tcp were open. When typing in the ip address of the machine on a web browser, I was able to gain access to the server with the company's directories.

02

Achievements

I was able to identify the IP address and the exposed services of the target VM.
I was also able to gain access to sensitive information and was able to discover a path to a secret folder.



03


```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-25 09:11 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.55 seconds
root@Kali:~#
```

Exploitation: Authentication Management

01

Tools & Processes

I exploited the vulnerability by using Brute Force Attack on the password for the hidden directory by using Hydra. I used Ashton's name, ran the Hydra attack against the directory. The tool I used to crack the hashed password I used both; the CrackStation website and John-the-ripper.

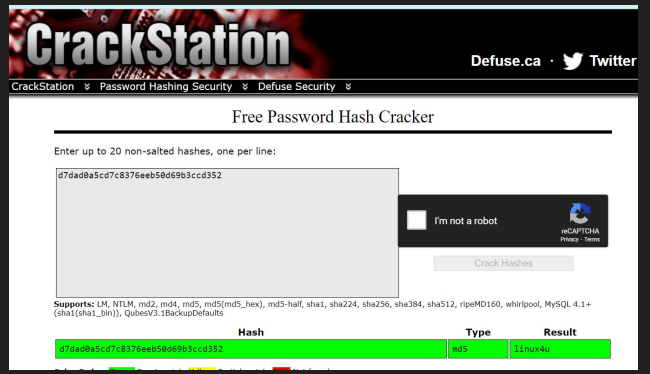
02

Achievements

The exploitation provided me with the username of 'ashton' as well with the password 'leopoldo'

03

```
root@Kali:/# john --format=raw-md5 ryans_haash
Created directory: /root/.john
stat: ryans_haash: No such file or directory
root@Kali:/# john --format=raw-md5 ryans_hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
linux4u          (?)
1g 0:00:00:24 DONE 3/3 (2022-07-25 13:29) 0.04149g/s 30498Kp/s 30498Kc/s 30
498KC/s linjbdi..linlklk
Use the "--show --format=Raw-MD5" options to display all of the cracked pas
swords reliably
Session completed
root@Kali:/#
```




```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 4] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-25 10:05:52
root@Kali:/#
```

Exploitation: LFI Vulnerability

01

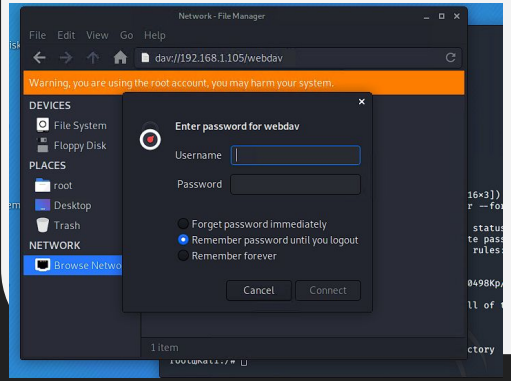
Tools & Processes

I exploited the vulnerability by using msfvenom and meterpreter to deliver a payload onto the vulnerable machine; the Capstone Server.

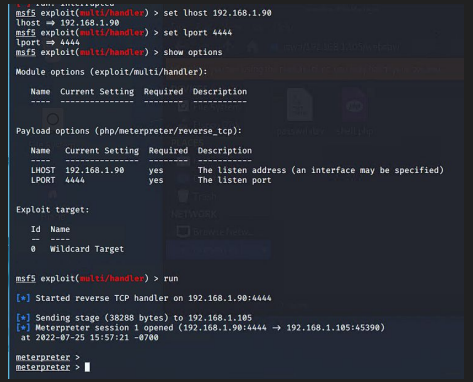
02

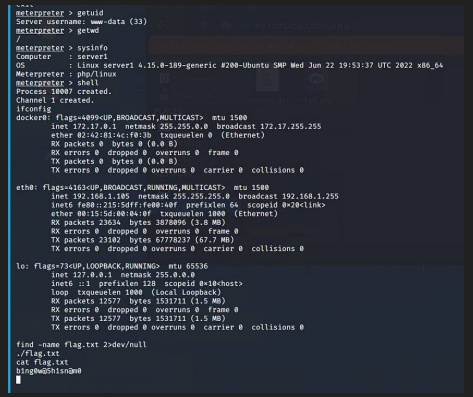
Achievements

By using the multi/handler exploit, I was successfully able to get access to the machine's shell.



03





Blue Team
Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?

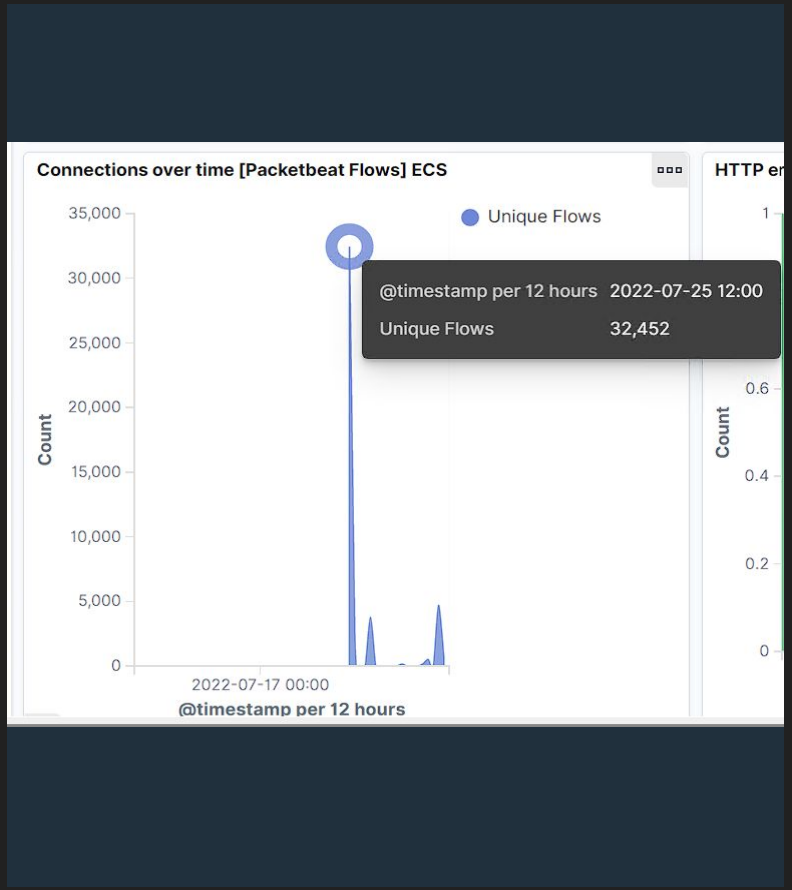
  07/25/2022 @12:00

- How many packets were sent, and from which IP?

  32,452 from the source IP 192.168.1.90

- What indicates that this was a port scan?

  The sudden peaks in network traffic indicate that this was a port scan.



Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,262
http://127.0.0.1/server-status?auto=	3,853
http://192.168.1.105/webdav	160
http://192.168.1.105/webdav/passwd.dav	29
http://snnmnkxdhflwgthqismb.com/post.php	28

Export: Raw Formatted

- What time did the request occur?

The request started at 11:00 on 07/25/2022

- How many requests were made?

About 16,262 requests were made to access the /secret_folder

- Which files were requested?

The /secret_folder contained hash that could be used to access the system using another employee's credentials which was Ryan.

- What did they contain?

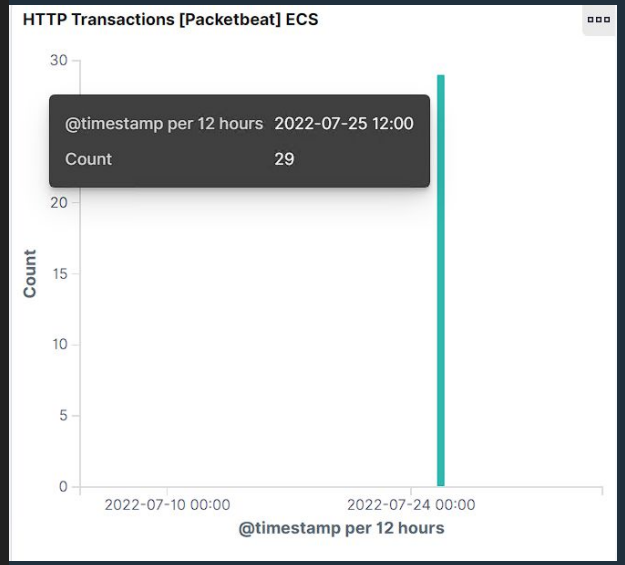
The /secret_folder allowed me to upload a payload – exploiting other vulnerabilities.

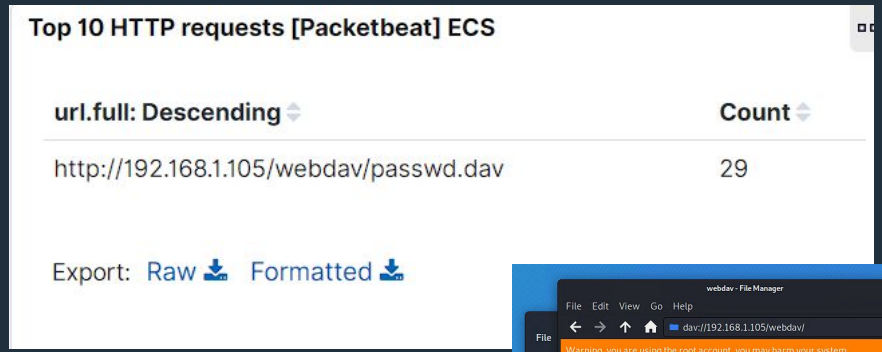
Analysis: Uncovering the Brute Force Attack

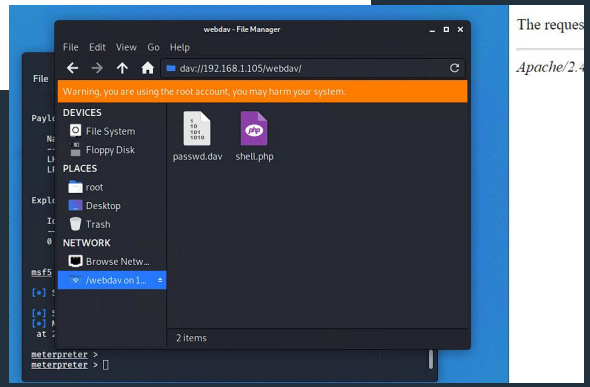
- How many requests were made in the attack? 16,262
- How many requests had been made before the attacker discovered the password? 16,262

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 29
- Which files were requested? Passwd.dav and shell.php







Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

Setting an alert be sent once 1000 connections occur in an hour.

What threshold would you set to activate this alarm?

Alert email and log when > 3 none port 403 or port 80 scans detected at the same timestamp from the IP occur

System Hardening

What configurations can be set on the host to mitigate port scans?

- Set server IPtables to drop packet traffic when thresholds are exceeded
- Ensure the firewall is regularly patched to minimize new zero-day attack
- Regularly run a system port scan to proactivity detect and audit any open ports
- Ensure the firewall detects and cuts off the scan attempt in real time.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

Setting an alert when future unauthorized access occur.

What threshold would you set to activate this alarm?

Maximum if 5 attempts per hour that would trigger an alert to be sent.

System Hardening

What configuration can be set on the host to block unwanted access?

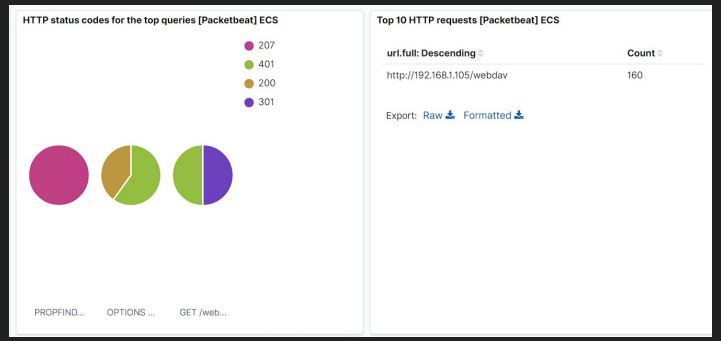
- Confidential folders that shouldn't be shared for public access
- Encrypting data that is contained within confidential folders
- Renaming folders that contains sensitive/private/company critical data
- Reviewing IP addresses that causes an alert to be sent: either whitelist or block the IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Setting an alarm that alerts if a 401 error is returned when detecting future brute force attacks.



What threshold would you set to activate this alarm?

Alert email and log when, on protected files and folders, > 5 Error (401) responses occur at any time OR any OK (200) responses occur from non-trusted IPs.

System Hardening

What configuration can be set on the host to block brute force attacks?

- Create a password policy that requires password complexity. Then compare the passwords to common passwords lists and prevent users from reusing historical passwords.
- Create a policy that locks out accounts for 30 mins after 5 unsuccessful attempts.
- Creating a blocked IP based on IP addresses that have 25 unsuccessful attempts in 4 months.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- Create a whitelist of trusted IP Addresses then review the list every 5 months if these users really need access
- Setting an alarm on HTTP request, in which it activates on any IP address that is trying to access the webDAV directory outside of those trusted IP addresses.

What threshold would you set to activate this alarm?

Alert email and log when requests are made, on protected files and folders, from non-trusted IPs.

System Hardening

What configuration can be set on the host to control access?

- Any access to the webDAV folder is only permitted by users with complex username and passwords when it comes to conjunction with other mitigation strategies.
- Ensuring that the firewall security policy prevents all other access and creating a whitelist of trusted IP addresses.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Setting an alert that can detect any traffic attempting to access port 4444.

Setting an alert for any files being uploaded into the /web/webDAV folder.

What threshold would you set to activate this alarm?

Alert email and log when “put” request methods are made, on protected folders, from non-trusted IPs

System Hardening

What configuration can be set on the host to block file uploads?

- Ensuring only necessary ports are open
- Blocking all IP addresses other than whitelisted IP addresses
- Giving permission to only read the /webDav folder, this prevent payloads from being uploaded


The End